GeekBrains

Урок 7 Тема 3

Применение и обход антиотладочных приемов. Часть 2

Реверс-инжиниринг

В этом видео

1. Принцип работы специальных функций WinAPI.
2. Самоотладка (self-debug).
3. Контроль целостности кода.
4. Подключение специальных плагинов.

GeekBrains

Способы обнаружения работы программы под отладчиком

- Измерение времени выполнения команд:
  - функция GetTickCount
  - инструкция RDTSC
- Поиск отладочных артефактов:
  - процессы
  - окна
- **Использование специальных функций WinAPI:**
  - **IsDebuggerPresent**
  - CheckRemoteDebuggerPresent
  - NtQueryInformationProcess
- Контроль целостности кода.

GeekBrains

Принцип работы специальных функций WinAPI

- IsDebuggerPresent
  - Флаг BeingDebugged из PEB
- CheckRemoteDebuggerPresent
  - Флаг BeingDebugged из PEB
- NtQueryInformationProcess
  - ProcessDebugPort из PROCESSINFOCLASS
  - ProcessDebugFlags из PROCESSINFOCLASS
  - ProcessDebugObjectHandle из PROCESSINFOCLASS

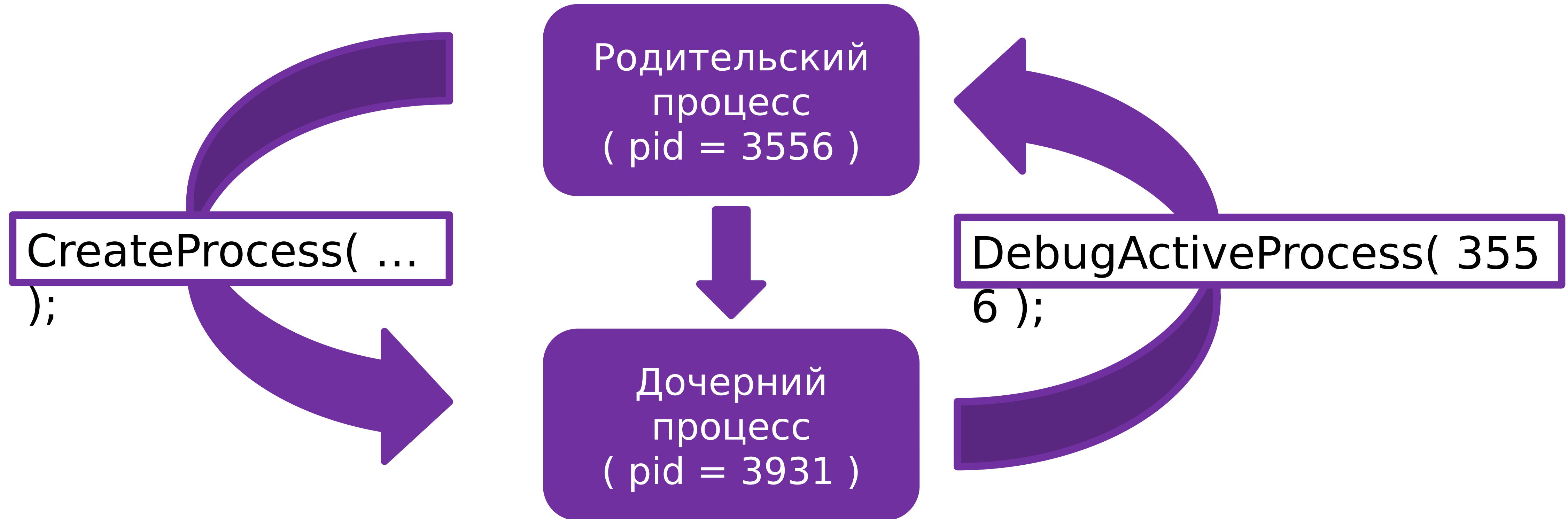
GeekBrains

Принцип работы функции NtQueryInformationProcess

```
NTQueryInformationProcess (
        in ProcessHandle,
        in ProcessInformationClass,
                // 0x07 - ProcessDebugPort
                // 0x1F - ProcessDebugFlags
                // 0x1E - ProcessDebugObjectHandle
        in ProcessInformation,
        in ProcessInformationLength,
        out ReturnLength
)
```

GeekBrains

Самоотладка (self-debug)



Способы обнаружения работы программы под отладчиком

- Измерение времени выполнения команд:
  - Функция GetTickCount
  - Инструкция RDTSC
- Поиск отладочных артефактов:
  - Процессы
  - Окна
- Использование специальных функций WinAPI:
  - IsDebuggerPresent
  - CheckRemoteDebuggerPresent
  - NtQueryInformationProcess
- **Контроль целостности кода.**

Использование специальных плагинов

- ScyllaHide

  https://github.com/x64dbg/ScyllaHide

- HideOD

  https://www.aldeid.com/wiki/OllyDbg/HideOD

- HideDebugger

  https://www.aldeid.com/wiki/OllyDbg/HideDebugger

Итоги

1. Узнали, как работают специальные функции WinAPI.
2. Познакомились с методом самоотладки (self-debug).
3. Поняли, как контроль целостности кода применяется для защиты от динамического анализа.
4. Узнали о специальных плагинах для отладчика OllyDbg.

GeekBrains